REMARKS

Prior to examination of the above-identified application, please consider the attached Substitute Specification (with marked-up version), together with replacement sheets of Figures 2A-2E.

Claims 1-10 have been cancelled and new claims 11-16 have been added. No new matter has been added.

Entry of this Preliminary Amendment is respectfully requested and deemed in order.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-1337 and please credit any excess fees to such deposit account.

Respectfully submitted,

LOWE HAUPTMAN GILMAN & BERNER, LLP

Kenneth M. Berner
Registration No. 37,093

1700 Diagonal Road, Suite 310
Alexandria, Virginia 22314
(703) 684-1111 KMB/jd
Facsimile: (703) 518-5499
Date: September 9, 2003

~~MARKED-UP VERSION~~

~~Renewing an Firmware of Computer System~~

~~ABSTRACT OF THE INVENTION~~

~~A system relates to the up-to-date of firmware for a computer memory system is disclosed. Firstly, a computer memory will be divided into as four portions using the function of this method accOrding to this present invention. Also, these four portions are employed as the following functions. The first portion is Initial Program, the second portion is Firmware (P 1), the third portion is a Backup Firmware (P2), the fourth portion is P1 Firmware Parameter, and finally the fifth portion is P2 firmware, respectively.~~

Method for Updating Firmware of Computer Device

ABSTRACT OF THE INVENTION

A method for updating firmware of computer device to write the newer firmware into the computer memory twice is disclosed. It includes dividing a memory of said computer device into five portions, wherein a initial program is saved in the first portion, a old firmware is saved in the second portion, a old backup firmware is saved in the third portion, the checksum of said old firmware is saved in the fourth portion and the checksum of said old backup firmware is saved in the fifth portion; executing said initial program in the first portion; writing a new firmware into the second portion from an external device for replacing said old firmware in the second portion; writing the checksum of said new firmware into the fourth portion from said external device; writing said new firmware into the third portion from said external device for replacing said old backup firmware in the third portion; writing the checksum of said new firmware into the fifth portion from said external device; and executing said new firmware in the second portion for operating said computer device.

BACKGROUND OF THE INVENTION

1.Field of the Invention

~~A system relates to the up-to-date of firmware for a computer system is disclosed, more particularly, the purpose firmware can be safely replaced instead of the original firmware.~~

The present invention generally relates to a method for updating firmware of computer device, and more particularly to a method for updating firmware of computer device to write the newer firmware into the computer memory twice.

2.Description of the Prior Art

~~The recent technology for upgrading firmware, is employed by using the combination application of computer software and firmware. Normally, the purpose firmware data of the computer system will be read whereby software operation and data transformation to the related system through transformation media.~~

~~Thus, the flow chart of computer system operation according to the prior art is shown as Figure 1. When the method starts, the prior firmware 10 will be removed as 11. Then the new firmware is set up into computer memory as 12. Thus the original firmware can be removed from the saved memory space of computer system using the above method. Consequentially the new firmware can be written into the memory space quickly.~~

~~However, if the computer system is suddenly stopped operating without the electrical power support, the computer system will be possibly destroyed. Especially, no~~

~~doubt, the sudden breakdown to a computer system at the time in the original firmware being upgraded, the computer system will be totally smashed by the above accident.~~

The current firmware upgrade technology is almost performed by the computer special software (initial program) along with the firmware. Said software will read the upgraded firmware data directly, and transmit it to the computer device via the variable interfaces. Such computer device will delete the original firmware in the computer memory first and write the new firmware data into its memory so as to finish upgrading and updating the firmware.

Figure 1 illustrates the above procedure. The original firmware has saved in the computer memory in the step 10 first. Then, in the step 11, the original firmware will be deleted from the computer memory, and finally the new firmware from external device will be installed to the computer memory in the step 12. However, many uncertain events during the step from 10 to 12, such as the power failure, will result in the damage to the computer device.

The disadvantage of this technology is that if the power failure or other uncertain events happen upon upgrading and updating the firmware and it incur the failure in writing the upgraded firmware, the original firmware in the memory can be destroyed or deleted, and the upgraded firmware is not completely installed in the computer memory yet. Therefore, such computer device will not function normally.

In general, the firmware, as the hybrid of the computer software and the hardware, is the hardware device with the predetermined program. In other words, the software recorded in the hardware is the firmware. For example, BIOS, recorded in the ROM on the motherboard should be implemented in order to turn on the computer before. Such BIOS, which can be modified only by the special burn-in machine, is one kind of the firmware. In addition to the ROM, the firmware can be stored in PROM, EPROM,

EEPROM or other programmable ROM. The programs recorded in ROM are usually named the microprograms. In present, the content of many firmwares in EPROM can be modified by the software (initial program). For example, the microprogram in the flash BIOS of the motherboard or modem can be modified by the initial program.

SUMMARY OF THE INVENTION

~~In accordance with the present invention, a method is provided for protecting and upgrading the firmware that substantially solves the above mentioned system error and possible faults to computer system. It certainly can be employed to necessity of the scanner as well. Therefore, the method of this present invention will be described as the below statement. The computer memory for saving firmware firstly will be divided as five portions. The five portions also can be indicated as the following.~~

~~The first portion is defined as an initialized program. The function of first portion is for protecting recent firmware situation and processing the movement of prior edition firmware and then installing new edition firmware into computer memory. It can be guaranteed that this initialized program never been not modified when movement and installing is under operation. Then, the second portion is a real firmware for controlling computer systems, which provides a new edition firmware loading. The third portion is a backup firmware of computer system. This portion is always correct and will be executed. Even though a new edition firmware is failed to install into the computer memory, the third portion still can repair the effort of third portion of firmware. Finally, the fourth portion and the fifth portion can save the parameter of the second and the third portion of firmware, such as the volume of computer files and the value of checksum.~~

~~When the firmware is under upgraded process, the second portion of firmware can be successfully updated if there is no error happened. The initialized program will backup the second portion into the third portion of firmware. When the errors happen under upgraded process, the initialized program will write back the backup file of the third portion to the second portion. Therefore, the computer system under operation still can recover the original firmware of original system, even though the errors happen under upgraded process. It can guarantee the system is under a normal condition. Also, it can set up the firmware under the safety condition. Of course, the parameter of all new five portions will.be successfully renewed.~~

In the light of the state of the art described above, it is an object of the present invention to provide a method for updating firmware of computer device which is immune to the problems of the conventional method for updating firmware of computer device. A newer firmware from external device must be written into the computer memory twice for avoiding the problem that the computer device can be not operated normally because the original firmware of the computer device has been deleted already but the newer firmware is not installed successfully into the computer memory yet.

In view of the above and other objects which will become apparent as the description proceeds, there is provided according to a general aspect of the present invention a method for updating firmware of computer device comprises dividing a memory of said computer device into five portions, wherein a initial program is saved in the first portion, a old firmware is saved in the second portion, a old backup firmware is saved in the third portion, the checksum of said old firmware is saved in the fourth portion and the checksum of said old backup firmware is saved in the fifth portion; executing said initial program in the first portion; writing a new firmware into the second portion from an external device for replacing said old firmware in the second portion; writing the checksum of said new firmware into the fourth portion from said external device; writing said new firmware into the third portion from said external device for

replacing said old backup firmware in the third portion; writing the checksum of said new firmware into the fifth portion from said external device; and executing said new firmware in the second portion for operating said computer device.

Based on the idea described above, wherein said computer device includes a scanner.

Based on the aforementioned idea, wherein the step of executing said initial program further comprises verifying the correctness of said old firmware program in the second potion by checking the checksum of said old firmware in the fourth potion; verifying the correctness of said old backup firmware program in the third potion by checking the checksum of said old firmware in the fifth potion; and verifying the identity of said old firmware program and said old backup firmware program.

Based on the idea described above, wherein the step of verifying the correctness of said old firmware program further comprises writing said old backup firmware program in the third portion into the second portion for renew said old firmware program when said old firmware program is defective; and writing the checksum of said old backup firmware program in the fifth portion into the fourth portion for renew the checksum of said old firmware program.

Based on the aforementioned idea, wherein the step of verifying the correctness of said old backup firmware program further comprises writing said old firmware program in the second portion into the third portion for renew said old backup firmware program when said old backup firmware program is defective; and writing the checksum of said old firmware program in the fourth portion into the fifth portion for renew the checksum of said old backup firmware program.

Based on the idea described above, wherein the step of verifying the identity of said old firmware program and said old backup firmware program further comprises writing said old backup firmware program in the third portion into the second portion for renew said old firmware program when said old backup firmware program is different from said old firmware program; and writing the checksum of said old backup firmware program in the fifth portion into the fourth portion for renew the checksum of said old firmware program.

BRIEF DESCRIPTION OF THE DRAWINGS

~~Further details of the present invention will be apparent to the those who skilled in the art by reference to the exemplary embodiment in the drawing in which:~~

~~Figure 1 illustrates the flow chart of the conventional technique according to the prior art;~~

~~Figure 2 illustrates the flow chart of this method according to the present invention; and~~

~~Figure 3 illustrates the relationship between the five conditions according to the present invention.~~

~~Table 1 illustrates the four portions of the memory of computer system according to this present embodiment.~~

The foregoing aspects and many of the attendant advantages of this invention will become more readily appreciated as the same becomes better understood by reference to the following detailed description, when taken in conjunction with the accompanying drawings, wherein:

Figure 1 illustrates the flowchart of conventional updating firmware;

Figures 2A-2E illustrate the flowchart of preferred embodiment according to the present invention; and

Figure 3 illustrates the four conditions by referring to Figures 2B-2E.

DESCRIPTION OF THE PREFERRED EMBODIMENT

~~The method of the present invention is applied to a broad range of firmware related range and can be from a variety of related invention. The following description discusses several presently preferred embodiments of the method of the present invention as implemented in process, since the majority of currently available is fabricated in~~

foundry and the most commonly encountered applications of the present invention will involve problems from trial and errors method. Nevertheless, the present invention may also be advantageously employed in any sort of computer technology. Accordingly, application of the present invention is not only intended to be limited to those devices fabricated in silicon semiconductor materials, but also will include those fabricated in one or more of the available.

Thus, the following is a description of the present invention.

The invention will firstly be described with reference to one exemplary structure. Some variations will be described as well as advantages of the present invention. A preferred method of fabrication will then be discussed. It can be that the disclosure of a digital computer having a memory containing a program which is executed by the computer.

The preferred embodiment of this present invention will be described as the following. As Table 1, firstly, the computer memory will be divided as the following five portions. The first portion as Initial Program is not modified but fixed up. Also, this Initial Program will be executed when computer system starts.

Table 1:

Initial Program
Firmware (P1)
Backup Firmware (P2)
P1 Firmware Parameter
P2 Firmware Parameter

Then checksum value of first portion of this firmware is calculated and is compared with the parameter of fourth portion for checking if it is proper. Then, the second portion is Firmware P1, the third portion is Backup Firmware P2. The fourth portion will be P1 Firmware Parameter according to Table 1 and the fifth portion will be P2 Firmware Parameter according to Table 1. Figure 2 also shows the inter-relationship between the following four conditions.

Normally, referring with Figure 2, the first portion of this computer firmware is defined as an Initial Program so that this program will not be modified but will be fixed. Also, this first portion of firmware will be executed while the system starts. Then, the second portion of Firmware (P1) is read and is calculated. Thus, checksum value of Firmware P1 will be obtained. The above checksum value of Firmware P1 can be compared with the parameter of the fourth portion and can be check if it is correct. When the result is correct, the computer system can be continued.

Sequentially, as Figure 2, the third portion of Firmware (P2) is read and is calculated. Thus, checksum value of Firmware P2 will be obtained. The above checksum value of Firmware P2 can be compared with the parameter of the fifth portion and can be check if it is correct. When the result is correct, the computer system can be continued.

Thus, the third portion of Firmware P2 can be checked. Here, Firmware P1 will be error at the last operation for refreshing the firmware of computer system if Firmware P1 is incorrect. At this time, Initial Program should write back to Backup Firmware P2 to

Firmware P1 of the second portion. Then, the original computer program can be repaired so that the computer system can still run the correct operation.

It is shown as Figure 2, after checking Firmware P1, the Backup Firmware P2 will be sequentially checked. Firstly, Backup Firmware P2 can be read and calculated its checksum value by Initial Program. Then the result can be compared with the parameter of the fourth portion and fifth portion of firmware, so that the next checking can be executed if Backup Firmware P2 is correct. However, if Backup Firmware P2 is incorrect, it can be ensured that there are errors of Backup Firmware P2 happened at the last duplicating firmware process. Therefore, at the same time, Initial Program should write Firmware P1 of computer system into Backup Firmware P2 of computer system and should restart the computer system again in order to execute Backup Firmware P2 of computer system. It can keep Backup Firmware P2 saved as a corrected firmware.

After Firmware P1 and Backup Firmware P2 are ensured all correct, both of the firmware should be compared if they are the same. After Firmware P1 is successfully renewed, Backup Firmware P2 is not yet backed up due to accidents possibly happen to the computer system, such as short circuit. Therefore, if the result is different after the comparability between Firmware P1 and Backup P2, Firmware P1 will be backup to Backup Firmware P2. If Firmware P1 and Backup P2 are the same after the comparability, Initial Program will be removed to Firmware P1, which can process the normal operation for computer system. Especially, this invention can be employed to necessity of the scanner.

With reference to Figure 2, the second portion as Firmware P1, the function of this portion for the computer system is really for controlling the computer system. The

new firmware data will firstly be rewritten into this portion at any time when it is going to refresh the original firmware.

The third portion, as Backup Firmware (P2), this portion is for becoming as the backup file of the present firmware. Also, the main function of this portion is for reconstructing the data of Firmware P1 if Firmware P1 is wrong, as Figure 2.

The fourth portion, as P1 Firmware Parameter, this portion is for saving Firmware P1 and Backup Firmware P2 and their checksum value. The same with he fifth portion, as P2 Firmware Parameter, this portion is for saving Firmware P1 and Backup Firmware P2 and their checksum value. Also these portions will be provided for checking Firmware P1 and checking Backup Firmware P2 under Initial Program operation, as Figure 2.

After the above definition, some of possible conditions will happen in the preferred embodiment. Thus, the flow chart of this preferred embodiment will be processed under the following conditions and shown by Figure 3.

Figure 3 shows Condition 1, which is under a normal execution without writing new firmware into the computer memory and starting from legend 20 of Figure 3:

(1) Checking Firmware P1, as legend 21 of Figure 3, it will be proper due to without writing operation;

(2) Checking Backup Firmware P2, as legend 22 of Figure 3, it will be proper due to without writing operation;

(3) Checking if Firmware P1 and Backup Firmware P2 is the same, as legend 23 of Figure 3, it will be the same due to without writing operation; and

(4) Back up to Firmware P1 and Firmware P1 will be executed if there is no error happened, as legend 24 of Figure 3.

Condition 2 is also indicates as Figure 3. Firmware P1 is written into the computer memory but the written operation is failed, so that the process is started from legend 20 of Figure 3:

(1) Checking if Firmware P1 is correct, as legend 21 of Figure 3, it could be wrong due to written operation is failed;

(2) Backup Firmware P2 is written into Firmware P1, as legend 25 of Figure 3. If it fails, it also can restart and go back to condition 3, as Figure 2, otherwise to be continued; and

(3) There is no error happened, Initial Program can be re-executed and it can go to Condition 1, as Figure 2.

Figure 3 illustrates Condition 3 as well. A changeable firmware, when Backup Firmware P2 is successfully written into the computer memory but backup operation is failed so that the process is started from legend 20 of Figure 3:

(1)Checking if Firmware P1 is correct, as legend 21 of Figure 3, it could be right due to successfully writing;

(2)Checking if Backup Firmware P2 is correct, as legend 22 of Figure 3 it could be wrong due to backup operation is failed, it needs a backup operation;

(3)Firmware P1 will be written into Backup Firmware P2, as legend 26 of Figure 3. If it fails, it also can restart and go back to condition 4, as Figure 2, otherwise to be continued; and

(4)There is no error happened, Initial Program will be re-executed and back to condition 1, as Figure 2.

Again, referring with Figure 3, Condition 4 for checking the purpose firmware is successfully written into the computer memory so that the process is started from legend 20 of Figure 3:

(1) Checking if Firmware P1 correct, as legend 21 of Figure 3, it is right due to a successful writing operation;

(2) Checking if Backup Firmware P2, as legend 22 of Figure 3, it is right without writing operation;

(3) Checking if Firmware P1 and Backup Firmware P2 are the same, as legend 23 of Figure 3. Firmware P1 and Backup Firmware P are different due to Firmware P1 is a changeable firmware but the Backup Firmware P2 is an original firmware, therefore Backup Firmware P2 will be backup;

(4) Firmware P1 is backup into Backup firmware P2, as legend 26 of Figure 3. It will go back to condition 4 if the backup operation is failed, as Figure 2. Then it can be continued if backup is successful; and

(5) There is no error happened, then Initial Program can be re-executed and back to condition 1, as Figure 2.

According to this preferred embodiment, this invention can perform method steps for operating a firmware that concludes the steps of the following. Also, this invention can be used to the scanner.

~~Firstly a memory of the machine is divided as five portions which are able to provide space for storing a plurality of computer readable program. Sequentially an initial program can be installed into a first portion of the memory of the machine and as a computer readable fixed program. Then removing a first firmware from the memory of the machine would be carried out. A second firmware is installed into a second portion of memory of the machine. A second firmware is backed up into a third portion of the memory of the machine. And finally, a plurality of parameter of the second firmware is installed into fourth portion of memory of the machine.~~

~~Finally, it is mentioned in the preferred embodiment, checking checksum of the firmware is the method for ensuring if the firmware is correct. Also, check checksum between any two of firmware will be the method for ensuring if both of the firmwares are the same. Therefore, in accordance with the present invention, a method is provided for protecting and upgrading firmware that substantially solves the above mentioned system error and possible faults to computer system. In addition, the computer system under operation still can recover the original firmware of original system, even though the errors happen under upgraded process. It can guarantee the system is under a normal condition. Also, it can set up the firmware under the safety condition. Of course, the parameter of all new five portions will be successfully renewed.~~

~~It is understood that various other modifications will be apparent to and can be readily made by those skilled in the art without departing from the scope and spirit of this invention. Accordingly, it is not intended that the scope of the claims appended hereto be limited to the description as set forth herein, but rather that the claims be construed as encompassing all the features of patentable novelty that reside in the present invention,~~

~~including all features that would be treated as equivalents thereof by those skilled in the art to which this invention pertains.~~

Some sample embodiments of the present invention will now be described in greater detail. Nevertheless, it should be recognized that the present invention can be practiced in a wide range of other embodiments besides those explicitly described, and the scope of the present invention is expressly not limited except as specified in the accompanying claims.

First, in the preferred embodiment to this invention, the computer memory should be divided into five portions as illustrated in Table 1. The Initial Program is saved to the first portion. The firmware program (P1) is saved to the second portion. The backup firmware program (P2) is saved to the third portion. The parameter of the P1 is saved to the fourth portion. The parameter of the P2 is saved to the fifth portion. This invention can also be applied to the scanner.

Table 1

First portion: initial program
Second portion: firmware program (P1)
Third portion: backup firmware program (P2)
Fourth portion: the parameter (checksum) of the P1
Fifth portion: the parameter (checksum) of the P2

As illustrated in Table 1, the initial program in the first portion is readable only. When the computer device starts, the initial program should be implemented first. Then, the firmware program (P1) in the second portion is read and the checksum of P1 is checked up. Such checksum will be verified in comparison with the parameter of the P1 in the fourth portion. If the verification passes, the firmware program (P1) is correct, and the whole procedure may continue.

If the firmware program (P1) is not correct upon the verification of the checksum of P1 and the parameter of the P1 in the fourth portion, the firmware program (P1) should be defective after the previous update. Then the initial program should read the backup firmware program (P2) in the third portion and write it into the second portion

in order to repair the original firmware program (P1) and the computer device can operate normally.

The verification of the backup firmware program (P2) in the third portion should continue after the successful verification on the firmware program (P1) in the second portion. The initial program will check up the checksum of the P2, and such checksum will be verified in comparison with the parameter of the P2 in the fifth portion. If the verification passes, the backup firmware program (P2) is correct, and the next step may be proceeded. If the verification fails, the backup firmware program (P2) should be defective. Then the initial program will read the firmware program (P1) in the second portion and write it into the third portion. Thus, the backup firmware program (P2) will be correct again.

The firmware program (P1) should be compared with the backup firmware program (P2) after the successful verification on the firmware program (P1) and the backup firmware program (P2). The reason is that the update step of the backup firmware (P2) may not be run due to the power failure after the successful update on the firmware program (P1). Therefore, if the firmware program (P1) is not the same with the backup firmware program (P2), the firmware program (P1) in the second portion should be duplicated to the third portion as the backup firmware program (P2). After the result regarding the comparison between the firmware program (P1) and the backup firmware program (P2) is identical, the implementation of the initial program will cease. And the firmware program (P1) should be implemented in order to operate the computer device. This invention can be applied to the scanner, too.

As illustrated in Table 1, the firmware program (P1) in the second portion is the main firmware to control the computer device. The newer firmware should be written into this portion upon updating the old firmware in the future.

As illustrated in Table 1, the backup firmware program (P2) in the third portion is the backup program of the main firmware to control the computer device. If the firmware program (P1) in the second portion is defective, then the backup firmware program (P2) in the third portion can be used to repair the defective firmware program (P1) and the computer device can operate normally again.

For the initial program verifies the correctness of the firmware program (P1) and the backup firmware program (P2), the parameters of the P1, P2 firmwares in the fourth and fifth portions, as illustrated in Table 1, are the checksums for the verification on the firmware program (P1) and the backup firmware program (P2).

Next, Figures 2A-2E and Figure 3 illustrate the flow chart of the preferred embodiment to this invention and also demonstrate the four conditions by referring to FIGs. 2B~2E as follows.

Please see the Figure 3. At the first condition, it is the normal condition that no firmware will be updated. The workflow of the initial program is as follows, (1) as shown in the step 21 in Figure 2B, this is to verify the correctness of the firmware program (P1) in the second potion by checking the checksum of such firmware in the fourth potion. If such firmware is not defective, it should be correct. (2) as shown in the step 22 in Figure 2B, it is to verify the correctness of the backup firmware program (P2) in the third potion by checking the checksum of such firmware in the fifth portion. If such firmware is not defective, it should be correct. (3) as shown in the step 23 in Figure 2B, this is to verify the identity of the firmware program (P1) with the backup firmware program (P2). (4) as shown in the step 24 in Figure 2B, there is no error under the above procedure, and the implementation of the firmware program (P1) in the second portion will be run to control the computer device.

Please revisit the Figure 3. The second condition is that the newer firmware should be written into the second portion of the computer memory but such operation fails. The workflow of the initial program is as follows, (1) as shown in the step 21 in Figure 2C, this is to verify the correctness of the firmware program (P1) in the second portion by checking the checksum of such firmware in the fourth portion. Due to the failure of the write operation, such firmware should be defective. (2) as shown in the step 25 in Figure 2C, the backup firmware program (P2) in the third portion will be restored into the firmware program (P1) in the second portion. If the write operation fails, the computer device should be rebooted, and the second condition may proceed. Otherwise, the next procedure as illustrated in Figure 2C may proceed. (3) as shown in the step 27 in Figure 2C, the parameter of the P2 in the fifth portion will be restored into the parameter of the P1 in the fourth portion. (4) as shown in Figure 2C, there is no error under the

above procedure, and the initial program will be implemented again in order to fulfill the first condition.

Please see Figure 3. The third condition is that the newer firmware is successfully written into the second portion of the computer memory but it fails to write into the backup firmware program of the third portion. The workflow of the initial program is as follows, (1) as shown in the step 21 in Figure 2D, this is to verify the correctness the firmware program (P1) in the second portion by checking the checksum of the such firmware in the fourth portion. Since the write operation finished successfully, such firmware should be correct. (2) as shown in the step 22 in Figure 2D, this is to verify the correctness of the backup firmware program (P2) in the third portion by checking the checksum of such firmware in the fifth portion. Due to the failure of the write operation, such firmware should be defective. (3) as shown in the step 26 in Figure 2D, the firmware program (P1) in the second portion will be restored into the backup firmware program (P2) in the third portion. If the write operation fails, the computer device should be rebooted, and the third condition may proceed. Otherwise, the next procedure as illustrated in Figure 2D may proceed. (4) as shown in the step 28 in Figure 2D, the parameter of the P1 in the fourth portion will be restored into the parameter of the P2 in the fifth portion. (5) as shown in Figure 2D, there is no error under the above procedure, and the initial program will be implemented again in order to fulfill the first condition.

Please see Figure 3. The fourth condition is that the newer firmware is successfully written into the second portion of the computer memory but it does not begin to write into the backup firmware program of the third portion due to the power failure or other reasons after the successful update on the firmware program (P1). The workflow of the initial program is as follows, (1) as shown in the step 21 in Figure 2E, this is to verify the correctness the firmware program (P1) in the second portion by checking the checksum of the such firmware in the fourth portion. Since the write operation finished successfully, such firmware should be correct. (2) as shown in the step 22 in Figure 2E, this is to verify the correctness of the backup firmware program (P2) in the third portion by checking the checksum of such firmware in the fifth portion. Due to the power failure, such firmware should be correct. (3) as shown in the step 23 in Figure 2E, this is to verify

the identity of the firmware program (P1) in the second portion with the backup firmware program (P2) in the third portion. The general method for verifying the identity of said two firmwares is to check the checksums of said two firmwares. Since the firmware program (P1) in the second portion is the newer firmware, and the backup firmware program (P2) in the third portion is the old firmware, the checksums of said two firmwares in the fourth and fifth portions are different. (4) as shown in the step 26 in Figure 2E, the firmware program (P1) in the second portion will be restored into the backup firmware program (P2) in the third portion. If the write operation fails, the computer device should be rebooted, and the fourth condition may proceed. Otherwise, the next procedure as illustrated in Figure 2E may proceed. (4) as shown in the step 28 in Figure 2E, the parameter of the P1 in the fourth portion will be restored into the parameter of the P2 in the fifth portion. (5) as shown in Figure 2E, there is no error under the above procedure, and the initial program will be implemented again in order to fulfill the first condition.

Although specific embodiments have been illustrated and described, it will be obvious to those skilled in the art that various modifications may be made without departing from what is intended to be limited solely by the appended claims.